

Report Documentation Page

*Form Approved
OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 24 OCT 2014	2. REPORT TYPE N/A	3. DATES COVERED		
4. TITLE AND SUBTITLE Cyber Intelligence Research Consortium Poster		5a. CONTRACT NUMBER		
		5b. GRANT NUMBER		
		5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) McAllister /Jay		5d. PROJECT NUMBER		
		5e. TASK NUMBER		
		5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)		
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.				
13. SUPPLEMENTARY NOTES The original document contains color images.				
14. ABSTRACT				
15. SUBJECT TERMS				
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 1	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified			

Cyber Intelligence Research Consortium

Advancing the art and science of cyber intelligence

The Consortium is a member-funded initiative that researches and develops technical solutions and analytical practices to help people make better judgments and quicker decisions with cyber intelligence.

Consortium Offerings to Members

	Steering Committee: Guide Consortium activities and plan for future success
	Cyber Threat Baseline: Anonymized research of members' cyber threat environments to identify common challenges and associated best practices
	Tradecraft Labs: Workshops to advance cyber intelligence capabilities and showcase relevant technologies
	Implementation Frameworks: How-to guides for navigating key analytical practices and technologies
	Crisis Simulation: Capture-the-flag exercise to apply analytical techniques and technologies to a simulated cyber attack
	Intelligence Insights: Biweekly emails and bimonthly newsletters on topics relevant to the practice of cyber intelligence

Reporting and Feedback

Offers courses of action to enhance decision making

- Represents the communication of and subsequent responses to cyber intelligence
- Takes into account audience background and technical expertise



Reporting & Feedback

Environmental Context

Provides scope for the analytical effort

- Highlights the importance of context - technical and nontechnical, internal and external to an organization



Environmental Context

Macroanalysis

Assesses the strategic implications of a cyber issue

- Adds perspective, context, and depth
- Enables proactive and predictive intelligence
- Provides appropriate insight for technical and nontechnical audiences



Macroanalysis

Analytical Acumen

Facilitates timely, actionable, and accurate intelligence on a cyber issue

- Conceptualizes an analyst's interactions with the other components
- Represents analytical tradecraft—the 'art' and 'science' of doing cyber intelligence analysis



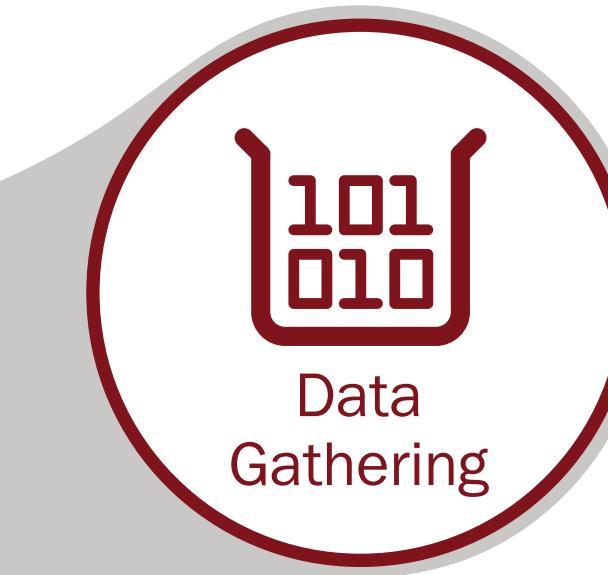
Analytical Acumen



Consortium Conceptual Framework

Cyber Intelligence: the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making.

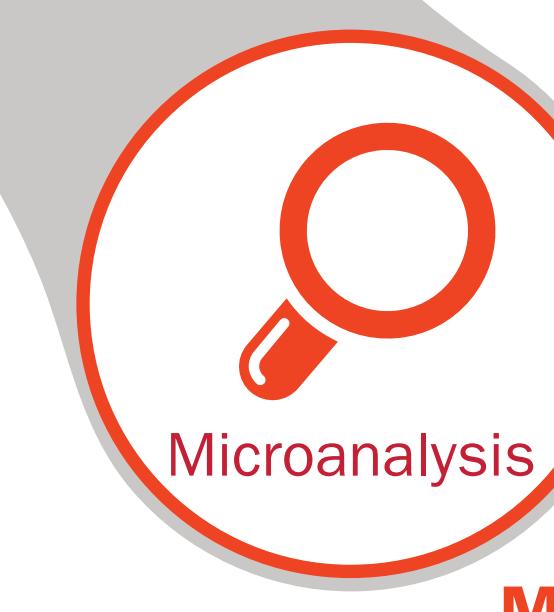
This framework puts this definition into practice. It emphasizes the rigor, agility, and creativity needed to analyze threats in the complex and ever-changing cyber domain.



Data Gathering

Acquires and aligns data for analysis

- Asks the right questions to get the right data, and the right amount
- Relies on domain expertise (self and others) and technology



Microanalysis

Microanalysis

Assesses the functional implications of the cyber issue

- Examines the issue's nature, ability, and quality
- Enables reactive intelligence